CyberSPAIS
Security Privacy & Assurance of Information Systems

CyberSPAIS
Security Privacy & Assurance of Information Systems

CISSP Overview

- Who Is Eligible for This Course?
  - Working IT professionals having at least 5 years of industry experience.

- Course Duration
  - 1.25 Months (48 Hours)

- Course Syllabus
  - General Security Concepts
  - Threats, Vulnerabilities, and Mitigations
  - Security Architecture
  - Security Operations
  - Security Program Management and Oversight

- Why Training @CyberSPAIS?
  - Job Oriented Industry Relevant Curriculum
  - Based On Latest Cyber Security Topics & Trends
  - 100% Assistance for Placements & Internships
  - Industry Experienced & Certified Trainer
  - Concepts Explained with Industry Scenarios
  - Comprehensive Hands-on Sessions & Labs
  - Regular Module Wise Assessments & Evaluations
  - Cybersecurity Projects & Internships
  - Thorough Preparation – Job Interview & Soft Skills
  - Arrangement To Write Certification Exams
  - Among The Top Cybersecurity Institutes in Kerala

- Launch a successful cybersecurity career
  - Develop a core foundation of essential skills, paving the way for a fulfilling career.
  - More job roles use Security+ for baseline cybersecurity skills than any other certification in the industry.

- Assess on-the-job skills
  - Security+ is the most widely adopted ISO/ANSI-accredited early career cybersecurity certification on the market with hands-on, performance-based questions on the certification exam.
  - These practical questions assess your ability to effectively problem solve in real-life situations and demonstrate your expertise to potential employers immediately.

- Embrace the latest trends
  - Understand and use the most recent advancements in cybersecurity technology, terms, techniques, and tools.

- By acquiring early career skills in the latest trends such as automation, zero trust, risk analysis, operational technology, and IoT, you will be well-equipped to excel in the ever-evolving cybersecurity landscape.

- About the exam
  - The new CompTIA Security+ (SY0-701) represents the latest and greatest in cybersecurity, covering the most in-demand skills related to current threats, automation, zero trust, IoT, risk – and more.
  - Once certified, you will understand the core skills needed to succeed on the job – and employers will notice too.
  - The Security+ exam verifies you have the knowledge and skills required to:
    - Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.
    - Monitor and secure hybrid environments, including cloud, mobile, Internet of Things (IoT), and operational technology.
    - Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.
    - Identify, analyze, and respond to security events and incidents.
    - CompTIA Security+ is compliant with ISO 17024 standards and approved by the U.S. DoD to meet Directive 8140.03M requirements.
    - Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program.
    - Over 3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

- What Skills Will You Learn?
  - General Security Concepts
    - Includes key cybersecurity terminology and concepts up front to provide a foundation for security controls discussed throughout the exam.
  - Threats, Vulnerabilities & Mitigations
    - Focuses on responding to common threats, cyberattacks, vulnerabilities, and security incidents and appropriate mitigation techniques to monitor and secure hybrid environments.
  - Security Architecture
    - Includes security implications of different architecture models, principles of securing enterprise infrastructure, and strategies to protect data.
  - Security Operations
    - Includes applying and enhancing security and vulnerability management techniques, as well as security implications of proper hardware, software, and data management.

- Security Program Management & Oversight
  - Updated to better reflect the reporting and communication skills required for Security+ job roles relating to governance, risk management, compliance, assessment, and security awareness.

- Exam Details
  - Exam Code
    - SY0-701
  - Launch Date
    - November 7, 2023
  - Exam Description
    - The CompTIA Security+ certification exam will verify the successful candidate has the knowledge and skills required to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions; monitor and secure hybrid environments, including cloud, mobile, and IoT; operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance; identify, analyze, and respond to security events and incidents
  - Number of Questions
    - Maximum of 90 questions
  - Type of Questions
    - Multiple choice and performance-based
  - Length of Test
    - 90 minutes
  - Passing Score
    - 750 (on a scale of 100-900)
  - Recommended Experience
    - CompTIA Network+ and two years of experience working in a security/ systems administrator job role
  - Languages
    - English, with Japanese, Portuguese, and Spanish to follow
  - Testing Provider
    - Pearson VUE
  - Exam Fees
    - USD 404 + Taxes

- Certification Renewal
  - Keep your certification up to date with CompTIA's Continuing Education (CE) program. It's designed to be a continued validation of your expertise and a tool to expand your skillset. It's also the ace up your sleeve when you're ready to take the next step in your career.
  - Get the most out of your certification
    - Information technology is an incredibly dynamic field, creating new opportunities and challenges every day. Participating in our Continuing Education program will enable you to stay current with new and evolving technologies and remain a sought-after IT and security expert.
  - The CompTIA Continuing Education program
    - Your CompTIA Security+ certification is good for three years from the day of your exam.

- The CE program allows you to extend your certification in three-year intervals through activities and training that relate to the content of your certification.
- Like Security+ itself, CompTIA Security+ CE also carries globally-recognized ISO/ANSI accreditation status.

- It's easy to renew
  - You can participate in a number of activities and training programs, including higher certifications, to renew your CompTIA Security+ certification.
  - Complete CertMaster CE, an online, self-paced CE course, or collect at least 50 Continuing Education Units (CEUs) in three years, upload them to your certification account and Security+ will automatically renew.

CISSP®

Certified Information Systems Security Professional

ISC2 Certification

Certification **Exam Outline**

Effective Date: April 15, 2024

ISC2™

About CISSP

The Certified Information Systems Security Professional (CISSP) is the most globally recognized certification in the information security market. CISSP validates an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization.

The broad spectrum of topics included in the CISSP body of knowledge ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following eight domains:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Experience Requirements

Candidates must have a minimum of five years cumulative, full-time experience in two or more of the eight domains of the current CISSP Exam Outline. Earning a post-secondary degree (bachelors or masters) in computer science, information technology (IT) or related fields may satisfy up to one year of the required experience or an additional credential from the ISC2 approved list may satisfy up to one year of the required experience. Part-time work and internships may also count towards the experience requirement.

A candidate that doesn't have the required experience to become a CISSP may become an Associate of ISC2 by successfully passing the CISSP examination. The Associate of ISC2 will then have six years to earn the five years required experience. You can learn more about CISSP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/CISSP/experience-requirements.

Accreditation

CISSP was the first credential in the field of information security to meet the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

ISC2 has an obligation to its membership to maintain the relevancy of the CISSP. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the CISSP. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today's practicing information security professionals.

CISSP CAT Examination Information

The CISSP exam uses Computerized Adaptive Testing (CAT) for all English, German, Spanish-Modern, Japanese, Simplified Chinese exams. You can learn more about CISSP CAT at www.isc2.org/certificatons/CISSP-CAT.

Length of exam	3 hours
Number of items	100 - 150
Item format	Multiple choice and advanced innovative items
Passing grade	700 out of 1000 points
Exam language availability	Chinese, English, German, Japanese, Spanish
Testing center	ISC2 Authorized PPC and PVTC Select Pearson VUE Testing Centers

CISSP CAT Examination Weights

Domains	Average Weight
1. Security and Risk Management	16%
2. Asset Security	10%
3. Security Architecture and Engineering	13%
4. Communication and Network Security	13%
5. Identity and Access Management (IAM)	13%
6. Security Assessment and Testing	12%
7. Security Operations	13%
8. Software Development Security	10%
Total:	**100%**

Domain 1: Security and Risk Management

1.1 Understand, adhere to, and promote professional ethics

- ISC2 Code of Professional Ethics
- Organizational code of ethics

1.2 Understand and apply security concepts

- Confidentiality, integrity, and availability, authenticity, and nonrepudiation (5 Pillars of Information Security)

1.3 Evaluate and apply security governance principles

- Alignment of the security function to business strategy, goals, mission, and objectives
- Organizational processes (e.g., acquisitions, divestitures, governance committees)
- Organizational roles and responsibilities
- Security control frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Payment Card Industry (PCI), Federal Risk and Authorization Management Program (FedRAMP))
- Due care/due diligence

1.4 Understand legal, regulatory, and compliance issues that pertain to information security in a holistic context

- Cybercrimes and data breaches
- Licensing and Intellectual Property requirements
- Import/export controls
- Transborder data flow
- Issues related to privacy (e.g., General Data Protection Regulation (GDPR), California Consumer Privacy Act, Personal Information Protection Law, Protection of Personal Information Act)
- Contractual, legal, industry standards, and regulatory requirements

1.5 Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

1.6 Develop, document, and implement security policy, standards, procedures, and guidelines

1.7 Identify, analyze, assess, prioritize, and implement Business Continuity (BC) requirements

- Business impact analysis (BIA)
- External dependencies

1.8 Contribute to and enforce personnel security policies and procedures

- Candidate screening and hiring
- Employment agreements and policy driven requirements
- Onboarding, transfers, and termination processes
- Vendor, consultant, and contractor agreements and controls

1.9 Understand and apply risk management concepts

- Threat and vulnerability identification
- Risk analysis, assessment, and scope
- Risk response and treatment (e.g., cybersecurity insurance)
- Applicable types of controls (e.g., preventive, detection, corrective)
- Control assessments (e.g., security and privacy)
- Continuous monitoring and measurement
- Reporting (e.g., internal, external)
- Continuous improvement (e.g., risk maturity modeling)
- Risk frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Payment Card Industry (PCI))

1.10 Understand and apply threat modeling concepts and methodologies

1.11 Apply supply chain risk management (SCRM) concepts

- Risks associated with the acquisition of products and services from suppliers and providers (e.g., product tampering, counterfeits, implants)
- Risk mitigations (e.g., third-party assessment and monitoring, minimum security requirements, service level requirements, silicon root of trust, physically unclonable function, software bill of materials)

1.12 Establish and maintain a security awareness, education, and training program

- Methods and techniques to increase awareness and training (e.g., social engineering, phishing, security champions, gamification)
- Periodic content reviews to include emerging technologies and trends (e.g., cryptocurrency, artificial intelligence (AI), blockchain)
- Program effectiveness evaluation

Domain 2: Asset Security

2.1 Identify and classify information and assets

- Data classification
- Asset Classification

2.2 Establish information and asset handling requirements

2.3 Provision information and assets securely

- Information and asset ownership
- Asset inventory (e.g., tangible, intangible)
- Asset management

2.4 Manage data lifecycle

- Data roles (i.e., owners, controllers, custodians, processors, users/subjects)
- Data collection
- Data location
- Data maintenance
- Data retention
- Data remanence
- Data destruction

2.5 Ensure appropriate asset retention (e.g., End of Life (EOL), End of Support)

2.6 Determine data security controls and compliance requirements

- Data states (e.g., in use, in transit, at rest)
- Scoping and tailoring
- Standards selection
- Data protection methods (e.g., Digital Rights Management (DRM), data loss prevention (DLP), cloud access security broker (CASB))

Domain 3: Security Architecture and Engineering

3.1 Research, implement and manage engineering processes using secure design principles

- Threat modeling
- Least privilege
- Defense in depth
- Secure defaults
- Fail securely
- Segregation of Duties (SoD)
- Keep it simple and small
- Zero trust or trust but verify
- Privacy by design
- Shared responsibility
- Secure access service edge

3.2 Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)

3.3 Select controls based upon systems security requirements

3.4 Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

- Client-based systems
- Server-based systems
- Database systems
- Cryptographic systems
- Industrial Control Systems (ICS)
- Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- Distributed systems
- Internet of Things (IoT)
- Microservices (e.g., application programming interface (API))
- Containerization
- Serverless
- Embedded systems
- High-Performance Computing systems
- Edge computing systems
- Virtualized systems

3.6 Select and determine cryptographic solutions

- Cryptographic life cycle (e.g., keys, algorithm selection)
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)
- Public key infrastructure (PKI) (e.g., quantum key distribution)
- Key management practices (e.g., rotation)
- Digital signatures and digital certificates (e.g., non-repudiation, integrity)

3.7 Understand methods of cryptanalytic attacks

- Brute force
- Ciphertext only
- Known plaintext
- Frequency analysis
- Chosen ciphertext
- Implementation attacks
- Side-channel
- Fault injection
- Timing
- Man-in-the-Middle (MITM)
- Pass the hash
- Kerberos exploitation
- Ransomware

3.8 Apply security principles to site and facility design

3.9 Design site and facility security controls

- Wiring closets/intermediate distribution facilities
- Server rooms/data centers
- Media storage facilities
- Evidence storage
- Restricted and work area security
- Utilities and heating, ventilation, and air conditioning (HVAC)
- Environmental issues (e.g., natural disasters, man-made)
- Fire prevention, detection, and suppression
- Power (e.g., redundant, backup)

3.10 Manage the information system lifecycle

- Stakeholders needs and requirements
- Requirements analysis
- Architectural design
- Development /implementation
- Integration
- Verification and validation
- Transition/deployment
- Operations and maintenance/sustainment
- Retirement/disposal

Domain 4: Communication and Network Security

4.1 Apply secure design principles in network architectures

- Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models
- Internet Protocol (IP) version 4 and 6 (IPv6) (e.g., unicast, broadcast, multicast, anycast)
- Secure protocols (e.g., Internet Protocol Security (IPSec), Secure Shell (SSH), Secure Sockets Layer (SSL)/ Transport Layer Security (TLS))
- Implications of multilayer protocols
- Converged protocols (e.g., Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP), InfiniBand over Ethernet, Compute Express Link)
- Transport architecture (e.g., topology, data/control/management plane, cut-through/store-and-forward)
- Performance metrics (e.g., bandwidth, latency, jitter, throughput, signal-to-noise ratio)
- Traffic flows (e.g., north-south, east-west)
- Physical segmentation (e.g., in-band, out-of-band, air-gapped)
- Logical segmentation (e.g., virtual local area networks (VLANs), virtual private networks (VPNs), virtual routing and forwarding, virtual domain)
- Micro-segmentation (e.g., network overlays/encapsulation; distributed firewalls, routers, intrusion detection system (IDS)/intrusion prevention system (IPS), zero trust)
- Edge networks (e.g., ingress/egress, peering)
- Wireless networks (e.g., Bluetooth, Wi-Fi, Zigbee, satellite)
- Cellular/mobile networks (e.g., 4G, 5G)
- Content distribution networks (CDN)
- Software defined networks (SDN), (e.g., application programming interface (API), Software-Defined Wide-Area Network, network functions virtualization)
- Virtual Private Cloud (VPC)
- Monitoring and management (e.g., network observability, traffic flow/shaping, capacity management, fault detection and handling)

4.2 Secure network components

- Operation of infrastructure (e.g., redundant power, warranty, support)
- Transmission media (e.g., physical security of media, signal propagation quality)
- Network Access Control (NAC) systems (e.g., physical, and virtual solutions)
- Endpoint security (e.g., host-based)

4.3 Implement secure communication channels according to design

- Voice, video, and collaboration (e.g., conferencing, Zoom rooms)
- Remote access (e.g., network administrative functions)
- Data communications (e.g., backhaul networks, satellite)
- Third-party connectivity (e.g., telecom providers, hardware support)

Domain 5: Identity and Access Management (IAM)

5.1 Control physical and logical access to assets

- Information
- Systems
- Devices
- Facilities
- Applications
- Services

5.2 Design identification and authentication strategy (e.g., people, devices, and services)

- Groups and Roles
- Authentication, Authorization and Accounting (AAA) (e.g., multi-factor authentication (MFA), password-less authentication)
- Session management
- Registration, proofing, and establishment of identity
- Federated Identity Management (FIM)
- Credential management systems (e.g., Password vault)
- Single sign-on (SSO)
- Just-In-Time

5.3 Federated identity with a third-party service

- On-premises
- Cloud
- Hybrid

5.4 Implement and manage authorization mechanisms

- Role-based access control (RBAC)
- Rule-based access control
- Mandatory access control (MAC)
- Discretionary access control (DAC)
- Attribute-based access control (ABAC)
- Risk-based access control
- Access policy enforcement (e.g., policy decision point, policy enforcement point)

5.5 Manage the identity and access provisioning lifecycle

- Account access review (e.g., user, system, service)
- Provisioning and deprovisioning (e.g., on /off boarding and transfers)
- Service accounts management
- Role definition and transition (e.g., people assigned to new roles)
- Privilege escalation (e.g., use of sudo, auditing its use)

5.6 Implement authentication systems

Domain 6: Security Assessment and Testing

6.1 Design and validate assessment, test, and audit strategies

- Internal (e.g., within organization control)
- External (e.g., outside organization control)
- Third-party (e.g., outside of enterprise control)
- Location (e.g., on-premise, cloud, hybrid)

6.2 Conduct security control testing

- Vulnerability assessment
- Penetration testing (e.g., red, blue, and/or purple team exercises)
- Log reviews
- Synthetic transactions/benchmarks
- Code review and testing
- Misuse case testing
- Coverage analysis
- Interface testing (e.g., user interface, network interface, application programming interface (API))
- Breach attack simulations
- Compliance checks

6.3 Collect security process data (e.g., technical and administrative)

- Account management
- Management review and approval
- Key performance and risk indicators
- Backup verification data
- Training and awareness
- Disaster recovery (DR) and Business Continuity (BC)

6.4 Analyze test output and generate report

- Remediation
- Exception handling
- Ethical disclosure

6.5 Conduct or facilitate security audits

- Internal (e.g., within organization control)
- External (e.g., outside organization control)
- Third-party (e.g., outside of enterprise control)
- Location (e.g., on-premises, cloud, hybrid)

Domain 7: Security Operations

7.1 Understand and comply with investigations

- Evidence collection and handling
- Reporting and documentation
- Investigative techniques
- Digital forensics tools, tactics, and procedures
- Artifacts (e.g., data, computer, network, mobile device)

7.2 Conduct logging and monitoring activities

- Intrusion detection and prevention (IDPS)
- Security information and event management (SIEM)
- Continuous monitoring and tuning
- Egress monitoring
- Log management
- Threat intelligence (e.g., threat feeds, threat hunting)
- User and entity behavior analytics (UEBA)

7.3 Perform configuration management (CM) (e.g., provisioning, baselining, automation)

7.4 Apply foundational security operations concepts

- Need-to-know/least privilege
- Segregation of Duties (SoD) and responsibilities
- Privileged account management
- Job rotation
- Service-level agreements (SLA)

7.5 Apply resource protection

- Media management
- Media protection techniques
- Data at rest/data in transit

7.6 Conduct incident management

- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Remediation
- Lessons learned

7.7 Operate and maintain detection and preventative measures

- Firewalls (e.g., next generation, web application, network)
- Intrusion detection systems (IDS) and intrusion prevention systems (IPS)
- Whitelisting/blacklisting
- Third-party provided security services
- Sandboxing
- Honeypots/honeynets
- Anti-malware
- Machine learning and artificial intelligence (AI) based tools

7.8 Implement and support patch and vulnerability management

7.9 Understand and participate in change management processes

7.10 Implement recovery strategies

- Backup storage strategies (e.g., cloud storage, onsite, offsite)
- Recovery site strategies (e.g., cold vs. hot, resource capacity agreements)
- Multiple processing sites
- System resilience, high availability (HA), Quality of Service (QoS), and fault tolerance

7.11 Implement disaster recovery (DR) processes

- Response
- Personnel
- Communications (e.g., methods)
- Assessment
- Restoration
- Training and awareness
- Lessons learned

7.12 Test disaster recovery plans (DRP)

- Read-through/tabletop
- Walkthrough
- Simulation
- Parallel
- Full interruption
- Communications (e.g., stakeholders, test status, regulators)

7.13 Participate in Business Continuity (BC) planning and exercises

7.14 Implement and manage physical security

- Perimeter security controls
- Internal security controls

7.15 Address personnel safety and security concerns

- Travel
- Security training and awareness (e.g., insider threat, social media impacts, two-factor authentication (2FA) fatigue)
- Emergency management
- Duress

Domain 8: Software Development Security

8.1 Understand and integrate security in the Software Development Life Cycle (SDLC)

- Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps, Scaled Agile Framework)
- Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))
- Operation and maintenance
- Change management
- Integrated Product Team

8.2 Identify and apply security controls in software development ecosystems

- Programming languages
- Libraries
- Tool sets
- Integrated Development Environment
- Runtime
- Continuous Integration and Continuous Delivery (CI/CD)
- Software configuration management (CM)
- Code repositories
- Application security testing (e.g., static application security testing (SAST), dynamic application security testing (DAST), software composition analysis, Interactive Application Security Test (IAST))

8.3 Assess the effectiveness of software security

- Auditing and logging of changes
- Risk analysis and mitigation

8.4 Assess security impact of acquired software

- Commercial-off-the-shelf (COTS)
- Open source
- Third-party
- Managed services (e.g., enterprise applications)
- Cloud services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

8.5 Define and apply secure coding guidelines and standards

- Security weaknesses and vulnerabilities at the source-code level
- Security of application programming interfaces (API)
- Secure coding practices
- Software-defined security

Additional Examination Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at www.isc2.org/certifications/References.

Examination Policies and Procedures

ISC2 recommends that candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at isc2.org/register-for-exam.

Legal Info

For any questions related to ISC2's legal policies, please contact the ISC2 Legal Department at legal@isc2.org.

Any Questions?

Contact ISC2 Candidate Services in your region:

Americas
Tel: +1.866.331.ISC2 (4722), press 1
Email: membersupport@isc2.org

Asia-Pacific
Tel: +(852) 5803-5662
Email: isc2asia@isc2.org

Europe, Middle East and Africa
Tel: +44 (0)203-960-7800
Email: info-emea@isc2.org

CISSP®

Certified Information Systems Security Professional

ISC2 Certification

The Ultimate Guide to the CISSP

Achieve the world's premier cybersecurity leadership certification

ISC2™

Achieve more in your career

You prove every day that you have what it takes to secure critical assets. But our profession is always changing, and even the brightest minds can benefit from having a guide on the journey to success. ISC2 is here to help you discover the right path, create your plan and thrive throughout your career.

The Ultimate Guide to the CISSP covers everything you need to know about the world's premier cybersecurity leadership certification. Inside, learn how CISSP and ISC2 help distinguish you as a top-level cybersecurity expert.

Inside...

- Is CISSP right for me?
- CISSPs in the community
- CISSP fast facts
- Benefits of CISSP certification
- Benefits of ISC2 membership
- Exam overview
- Official training
- Pathway to certification
- CPE opportunities
- Continuing professional development

Is CISSP **right for me?**

As organizations continue to pursue digital transformation initiatives, the threat landscape is always expanding. Yet cybersecurity leadership talent is scarce. That's where CISSP from ISC2 comes in — to help fill the gap. Once certified, the opportunities for certified professionals are near limitless.

CISSP, a vendor-neutral cybersecurity credential, shows you have the knowledge to design, implement and manage a best-in-class cybersecurity program in any environment. Vendor-neutral credentials are sought by organizations to avoid the limitations and expense of vendor lock-in.

CISSP is particularly well-suited for information security professionals seeking to prove their understanding of cybersecurity strategy and hands-on implementation. It shows you have the advanced knowledge and technical skills to design, develop and manage an organization's overall security posture.

As a first step – become an ISC2 Candidate

Begin your journey by joining ISC2, the world's leading cybersecurity professional organization. As a Candidate, you'll access many of the benefits our certified members enjoy, including 20% off online training and 30% - 50% off textbooks to help you on your path to CISSP certification. .

Sign up now. Your first year is free — no cost to you.*

*If you choose to renew after the first year, U.S. $50 due annually.

Acquire five years of experience

To qualify for the CISSP, candidates must have a minimum of five years cumulative full-time experience in two or more of the eight domains of the ISC2 CISSP Exam Outline.

If you don't yet have the required experience, you may become an Associate of ISC2 after successfully passing the CISSP exam. The Associate of ISC2 will then have six years to earn the experience needed for the CISSP certification.

Discover your path

See "Pathway to certification" for more information.

Certified Information Systems Security Professional

ISC2 Certification

Jobs that typically use or require CISSP certification

- Chief Information Officer
- Chief Information Security Officer
- Chief Technology Officer
- Compliance Manager/Officer
- Director of Security
- Information Architect
- Information Manager/Information Risk Manager or Consultant
- IT Specialist/Director/Manager
- Network/System Administrator
- Security Administrator
- Security Architect/Security Analyst
- Security Consultant
- Security Manager
- Security Systems Engineer/Security Engineer

CISSPs in the community

"CISSP is recognized worldwide as the gold standard. The whole premise of it is not just passing the exam but demonstrating you have the verifiable experience to perform at a high level. The ISC2 Code of Ethics is important. The ongoing CPE requirement is tough, but it helps make sure your skills stay up to date. It all adds up to a very credible certification."

Angus Macrae
Head of Cybersecurity
King's Service Centre, Cornwall, England

"CISSP gives you a lot of street credibility with the people who do this for a living because they all understand what it is. It's definitely an important designation to have on your calling card. I see it as the gold standard in cybersecurity. It's the most-recognized credential in the security community."

Theresa Grafenstine
Global Chief Auditor, Technology
Citi, Wilmington, DE, USA

"When I passed the CISSP exam, I gained access to the strong network of industry professionals at ISC2. I attend industry events to learn more about how my peers are dealing with cybersecurity challenges. The ISC2 Community online discussion board and local chapters have engaging presentations and workshops where you can focus on your skills."

Jason Lau
CISO
Crypto.com, Singapore

"The CISSP made me a stronger professional. It taught me that everything I was learning while working at one company was not going to work everywhere. Now I know what the standard is and how to identify the best framework. When I'm put in different and unfamiliar positions, I have a solid foundation from the CISSP that I can work from."

Christine Izuako
Founder and CEO, Cyber Pop-up
Chicago, IL

Become an ISC2 Candidate

You'll access a full range of benefits as you pursue the CISSP, including 20% off online training and 30% - 50% off textbooks to help you prepare. **Sign up now**.

CISSP **Fast facts**

Introduced in 1994

CISSPs are part of a network of more than 600,000 cybersecurity professionals

93% of CISSPs are lifers

ANAB/ANSI accredited

Computerized Adaptive Testing (CAT) introduced December 18, 2017

Most required security certification by hiring managers on LinkedIn

DoD-approved

ISC2 certified members work in more than 170 countries globally

Average CISSP Salary: U.S. $140,230

Shout-outs

RANKED #1 ON 'THE NEXT BIG THING' LIST as the certification survey respondents plan to earn in 2023. — *Certification Magazine*

Named one of the **TOP CERTIFICATIONS IN BEST INFORMATION SECURITY CERTIFICATIONS**

Named the **MOST VALUED CREDENTIAL AMONG EMPLOYERS** by a margin of 3 to 1

Repeatedly voted **'BEST PROFESSIONAL CERTIFICATION PROGRAM'** — *SC Magazine*

#1 SECURITY CREDENTIAL required by hiring managers on LinkedIn

Benefits of CISSP certification

Career opportunities and advancement
Raise visibility and credibility and create new career opportunities.

Credibility
Demonstrate a solid foundation to mitigate and respond to cyberthreats.

Membership in a strong peer network
Become an ISC2 member, unlocking exclusive resources, educational tools and peer-to-peer networking opportunities.

Expanded knowledge
Reach a deeper, better and broader understanding of the Exam Outline.

Versatile skills
Build vendor-neutral skills that can be applied to different technologies and methodologies.

Leadership
Develop a broad set of technical and nontechnical skills that job experience alone doesn't provide.

Higher salaries
Earn more. In 2023, Certification Magazine's annual survey lists an average salary of $140,230 (in U.S.) and $115,080 (globally).

Stronger skill set
Expand the skills and knowledge needed to fulfill organizational duties.

Benefits of **ISC2 membership**

Once you earn your CISSP, you'll become an ISC2 member and part of a professional community that never stops learning and growing. You'll also gain access to a full suite of benefits and resources for continuing education and development, many that will help you earn CPE credits to maintain your certification:

- Free online **continuing professional development** courses
- Discount on **ISC2 Certificates**
- Discount pricing for **ISC2 events** and industry events including **ISC2 Security Congress**
- Discounts on select publications including CBK books, practice test books and study guides
- Free access to **ISC2 webinars** on cybersecurity topics, tools and trends
- Invitation to join or start a **local ISC2 Chapter**
- **Volunteer opportunities**
- Access to the **Center for Cyber Safety and Education**
- Professional recognition through **ISC2 Global Achievement Awards**

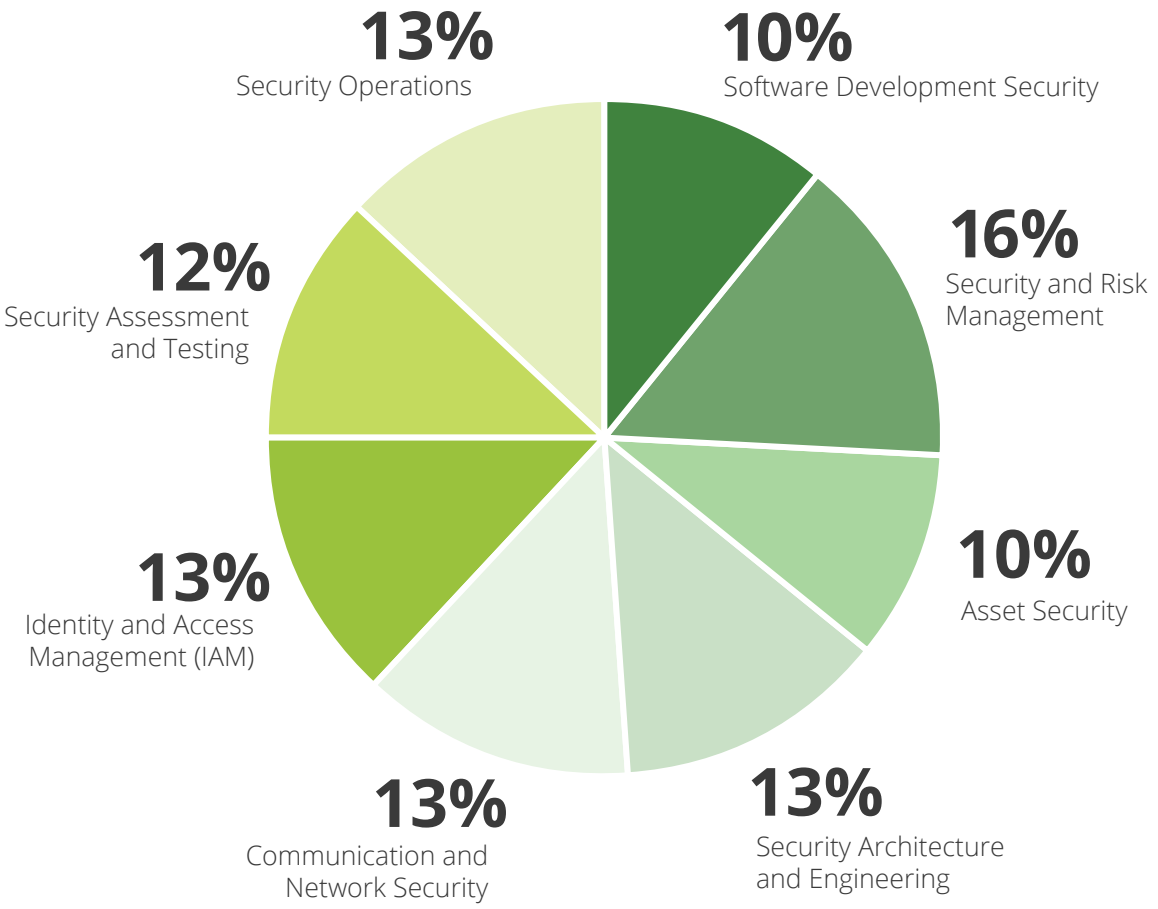
Sign up now to become an ISC2 Candidate

Your first year is free — no cost to you.* You'll enjoy most of these benefits as you prepare for certification — plus 20% off Online Self-Paced and Online Instructor-Led Training for CISSP.

*If you choose to renew after the first year, U.S. $50 due annually.

Exam overview

The CISSP exam evaluates expertise across eight security domains. (Think of domains as topics you need to master based on your professional experience and education.) Passing the exam proves you have the advanced knowledge and technical skills to effectively design, implement and manage a best-in-class cybersecurity program.



100-150

Number of items on the CISSP CAT (Computer Adaptive Testing) exam

3 hrs. Maximum amount of time for the CISSP CAT exam

700 Score you need out of 1,000 to pass the exam

View the CISSP **exam outline**.

Exam availability:
English, Chinese, German, Japanese and Spanish

Testing Centers:
ISC2 Authorized PPC and PVTC Select Pearson VUE Testing Centers

Official **training**

ISC2 offers Official Training for CISSP. Save 20% on Official ISC2 Training when you sign up to be an **ISC2 Candidate**.

Everyone has their own style of learning. That's why we offer three options to help guide you in CISSP certification. Experience new learning with recently enhanced Official ISC2 CISSP Training options. **Find training**.

1. **Online Self-Paced – Register now**
   Your self-guided tour toward certification — now featuring adaptive learning for a streamlined experience customized to each individual. Leveraging the power of AI, the training guides learners through a self-paced learning experience adapted to their individual needs.
   - Flexibility to study on your own time and at your own pace
   - Personalized learning that adapts to your needs
   - Interactive, engaging courseware
   - Analytics dashboard to track learning progress
   - Education Guarantee

2. **Online Instructor-Led – Register now**
   Progress through the course domain-by-domain with content that's organized to align specifically to the CISSP Exam Outline domains to be easier-to-follow in live sessions led by an ISC2 Authorized Instructor.
   - Live virtual instruction from an ISC2 Authorized Instructor
   - Virtual collaboration with classmates
   - Interactive, engaging courseware
   - New digital eTextbook
   - Addition of glossary
   - Key takeaway resources for each domain
   - Education Guarantee

3. **Classroom – Learn more**
   Your guided small group tour (10 or more students) toward certification
   - Learn in-person at your office or a private venue near you
   - Interact with an ISC2 Authorized Instructor and students
   - Coordinate training around your schedule

CISSP self-study tools

We offer a variety of **self-study tools** to supplement your coursework and reinforce key concepts. Choose from options for every schedule and learning style.

Pathway to certification

1 Become an ISC2 Candidate

Begin your journey by joining ISC2, the world's leading cybersecurity professional organization. As a candidate, you'll access many of the benefits our certified members enjoy, including 20% off training and 30% - 50% off textbooks to help you on your path to CISSP. **Sign up now**.

2 Obtain the required experience

To qualify for the CISSP, candidates must have a minimum of five years cumulative full-time experience in two or more of the eight domains of the ISC2 CISSP Exam Outline.

- **Domain 1:** Security and Risk Management
- **Domain 2:** Asset Security
- **Domain 3:** Security Architecture and Engineering
- **Domain 4:** Communication and Network Security
- **Domain 5:** Identity and Access Management (IAM)
- **Domain 6:** Security Assessment and Testing
- **Domain 7:** Security Operations
- **Domain 8:** Software Development Security

If you don't yet have the required experience, you may become an Associate of ISC2 after successfully passing the CISSP exam. The **Associate of ISC2** will then have six years to earn the experience needed for the CISSP certification.

Pathway to certification

3 Study for the exam

Many **self-study resources** are available from ISC2 – the creator and keeper of the CISSP CBK – to help you prepare with confidence. Some CISSP candidates pass the exam with self-study, and many choose to attend an **Official ISC2 Training** to review and refresh their knowledge before sitting for the exam.

4 Pass the exam

You have a maximum of three hours to complete the 100-150 item CISSP CAT exam. Ready to schedule your exam? **Register now** and get it on the calendar.

5 Get endorsed

After you pass the exam, you have nine months from the date of the exam to complete the **ISC2 endorsement process**.

6 Earn CPE credits

Once you are certified, you become a member of ISC2 and recertify every three years. Recertification is accomplished by earning continuing professional education (CPE) credits and paying an **annual maintenance fee (AMF)** to support ongoing development.

120 CPE credits over 3 years

(40 CPE credits recommended yearly)

U.S. $135 AMF

Members with multiple ISC2 certifications only pay a single AMF.

CPE opportunities

The CPE credit requirement helps you maintain your competencies following initial certification. By developing and enhancing skills through CPE activities, you make an important investment in yourself while increasing value to customers and employers.

Join webinars

- Think Tanks
- Security Briefings
- Knowledge Vault
- Security Congress

Read and write

- Read a book directly related to CISSP and submit a 150-word review
- Author an information security article published in a journal or magazine
- Review an educational white paper related to the CISSP

Attend trainings and events

- ISC2 Chapter meetings
- Prepare or attend an educational presentation related to the CISSP CBK domains
- ISC2 Skill-Builders – grow your knowledge with short-format learning on demand
- ISC2 Certificates – grow your skills with quick learning averaging just 3.5 hours per certificate that focuses on high demand subject matter
- Discount pricing for ISC2 events and industry events, including ISC2 Security Congress

Volunteer

- Become a Safe and Secure Online Ambassador and spread your knowledge about cyber safety in your community
- Volunteer to help develop ISC2 certification exams

Continuing **professional development**

ISC2 Certificates allow you to advance your skills in areas employers are seeking and provide pathways toward gaining the competencies you need for the journey to ISC2 certification.

- Our online **ISC2 CISO Leadership Certificates** focus on real-world applications of cybersecurity management principles from an executive management point of view.
- Our online **ISC2 Healthcare Certificates** focus on securing patient health information and navigating a complex regulatory environment.

Innovate, lead and transform cybersecurity across your organization with **ISC2 Executive Leadership Courses**, created by industry experts and available on demand. Broaden your skill set and break through barriers with actionable strategies that deliver measurable results both you and the board can get behind.

Our online **ISC2 Managing Zero Trust Data Risk Courses** cover the principles and requirements necessary to manage enterprise risks in a zero trust environment. Online on-demand courses include:

- Zero Trust Risk Management and Response
- Security within Zero Trust
- Communication for Zero Trust

Stay in front of the hottest topics and trends impacting your current role and your cybersecurity career with **ISC2 Cybersecurity Leadership Skill-Builders**, created by industry experts and available now on demand. Gain key perspectives on the fundamental concepts of cybersecurity and their real-world applications for executive- and board-level planning and decision-making.

CISSP

Certified Information Systems Security Professional

ISC2 Certification

Get in touch with us

For more information about CISSP certification and training, contact an Education Consultant in your region:

Americas — Phone: +1.866.331.4722 ext. 2, Email: **training@isc2.org**

Europe, Middle East and Africa — Phone: +44 203 960 7800, Email: **info-emea@isc2.org**

Asia-Pacific — Phone: +852.5803.5662, Email: **isc2asia@isc2.org**

About ISC2

ISC2 is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, ISC2 offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our association of candidates, associates and members, more than 600,000 strong, is made up of certified cyber, information software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – **The Center for Cyber Safety and Education**™. For more information on ISC2, visit **isc2.org**, follow us on **X**, or connect with us on **Facebook**, **LinkedIn** and **YouTube**.

ISC2

06/2024